**In the Claims**

1. (currently amended) A method of storing a digital asset in a data repository ~~for the purpose of providing efficient access to the data over~~ coupled to a network, said method comprising:

receiving, at the data repository, a broadcast cryptographic hash descriptor file identifier that identifies the digital asset;

determining whether the broadcast cryptographic hash descriptor file identifier is a ~~known~~ cryptographic hash descriptor file identifier known to the data repository;

when the broadcast cryptographic hash descriptor file is not known to the data repository, adding the broadcast cryptographic hash descriptor file identifier to a list of desired broadcast cryptographic hash descriptor file identifiers;

receiving, at the data repository, the [[a]] digital asset identified by the broadcast cryptographic hash descriptor file identifier;

generating a generated cryptographic hash descriptor file identifier from the ~~assembled asset~~ received digital asset; and

verifying that the generated cryptographic hash descriptor file identifier for the received digital asset matches the broadcast cryptographic hash descriptor file identifier.

2. (currently amended) A method as recited in claim 1, wherein adding the broadcast cryptographic hash descriptor file identifier to the list includes:

determining the number of times the broadcast cryptographic hash descriptor file identifier has been received at the data repository; and

determining whether to add the cryptographic hash descriptor file identifier to said list based upon said number of times.

3. (currently amended) A method as recited in claim 1, wherein receiving [[a]] the digital asset identified by the transmitted cryptographic hash descriptor file identifier includes:

receiving portions of said asset identified by the transmitted cryptographic hash descriptor file identifier at different times; and

assembling the portions of the asset into the complete asset.

4. (currently amended) A method as recited in claim 3, further comprising issuing a broadcast request for the digital asset corresponding to the broadcast cryptographic hash descriptor file identifier, and wherein the method further ~~comprising~~ comprises:

ending [[a]] the broadcast request for portions of ~~assets~~ the digital asset that have not been obtained.

5. (currently amended) A method as recited in claim 4, further comprising:

determining an amount of broadcast traffic on ~~a local~~ at least a portion of the network; and

determining whether to send the broadcast request based on the amount of broadcast traffic on the ~~local~~ at least a portion of the network.

6. (currently amended) A method as recited in claim 1, further comprising:

quarantining the asset while verifying that the generated cryptographic hash descriptor file identifier matches the broadcast cryptographic hash descriptor file identifier.

7. (currently amended) A method as recited in claim 1, wherein the data repository is a first data repository of a plurality of data repositories ~~configured serially are present on said~~ coupled to the network, ~~said~~ and wherein the method further ~~comprising~~ comprises:

comparing the cryptographic hash descriptor file identifier to a selection rule for the first data repository; and

determining whether to add the broadcast cryptographic hash descriptor file identifier to [[a]] the list of desired broadcast cryptographic hash descriptor file identifiers based on said selection rule.

8. (currently amended) A method as recited in claim 1, wherein said received asset is a descriptor file, said method further comprising:

opening the descriptor file to obtain a list of asset identifiers included therein; and

adding the list of asset identifiers to the list of desired broadcast cryptographic hash descriptor file identifiers.

9. (currently amended) A method as recited in claim 1, further comprising:

storing said received asset in said data repository; and

responding to a ~~network~~ request received over the network from ~~a network~~ another device for said stored asset by broadcasting the stored asset.

10. (currently amended) A method as recited in claim 1, further comprising:

responding to a ~~network~~ request, received over the network from ~~a network~~ another device, for a ~~stored~~ digital asset stored in the data repository by broadcasting portions of the stored asset; and

broadcasting the portions of the stored ~~file~~ asset before the entire asset is received at the data repository.

11. (currently amended) A data repository ~~on~~ to be coupled to a network, the data repository comprising:

an asset collector operative to:

receive, over the network, a broadcast cryptographic hash asset identifier,

add the broadcast cryptographic hash asset identifier to a list of desired broadcast cryptographic hash asset identifiers,

receive an asset identified by the broadcast cryptographic hash asset identifier,

verify the identity of the received asset by generating a generated cryptographic hash asset identifier from the ~~assembled asset~~ received asset, and

compare the generated cryptographic hash asset identifier to the broadcast cryptographic hash asset identifier;

an asset storage ~~memory for storing~~ device to store the received asset; and

an asset supplier ~~for supplying the file~~ to supply the stored asset to a network device that requests the asset.

12. (currently amended) A method of selectively storing data in a data repository and providing stored data from [[a]] the data repository over a network, said method comprising:

receiving, at the data repository, a broadcast cryptographic hash digital asset identifier;

determining whether the broadcast cryptographic hash asset identifier corresponds to a received asset that is stored in the data repository;

adding the broadcast cryptographic hash descriptor file identifier to a list of desired broadcast cryptographic hash descriptor file identifiers ~~if~~ when the broadcast cryptographic hash asset identifier does not correspond to a received asset that is stored in the data repository; and

broadcasting the received asset that is stored in the data repository ~~if~~ when the broadcast cryptographic hash asset identifier corresponds to a received asset that is stored in the data repository.

13. (currently amended) A method of deleting a digital asset in a data repository that includes an asset list that identifies the digital asset as being stored in the data repository, the method comprising:

receiving, at the data repository, a broadcast cryptographic hash descriptor file identifier;

adding the broadcast cryptographic hash descriptor file identifier to a list of files to be deleted;

comparing the broadcast cryptographic hash asset identifier to a generated cryptographic hash asset identifier ~~that represents~~ for ~~a known asset in an asset list~~ the digital asset; and

deleting the ~~known~~ digital asset from the asset list that identifies the digital asset as being stored in the data repository when the broadcast cryptographic hash asset identifier matches the generated cryptographic hash asset identifier.

14. (new) The method of claim 1, further comprising:

issuing a broadcast request over the network requesting the digital asset corresponding to the broadcast cryptographic hash descriptor file identifier.

15. (new) The method of claim 1, further comprising, after adding the broadcast cryptographic hash descriptor file identifier to the list of desired cryptographic hash descriptor file identifiers, issuing a broadcast request over the network requesting the digital asset corresponding to the broadcast cryptographic hash descriptor file identifier.